

Outline of HIPAA Security Rule Standards and Implementation Specifications

Administrative Safeguard Standards:

- Security Management Process
 - *Risk analysis (Required).*
 - *Risk management (Required).*
 - *Sanction policy (Required).*
 - *Information system activity review (Required).*
- Assigned Security Responsibility (Required)
- Workforce Security
 - *Authorization and/or supervision (Addressable)*
 - *Workforce clearance procedure (Addressable).*
 - *Termination procedures (Addressable)*
- Information Access Management
 - *Isolating health care clearinghouse functions (Required).*
 - *Access authorization (Addressable).*
 - *Access establishment and modification (Addressable).*
- Security Awareness and Training
 - *Security reminders (Addressable).*
 - *Protection from malicious software (Addressable).*
 - *Log-in monitoring (Addressable).*
 - *Password management (Addressable).*
- Security Incident Procedures
 - *Response and reporting (Required).*
- Contingency Plan
 - *Data backup plan (Required).*
 - *Disaster recovery plan (Required).*
 - *Emergency mode operation plan (Required).*
 - *Testing and revision procedures (Addressable).*
 - *Applications and data criticality analysis (Addressable).*
- Evaluation (Required)
- Business Associate Contracts and Other Arrangements
 - *Implementation specifications: Written contract or other arrangement (Required).*

Physical Safeguard Standards:

- Facility access controls
 - *Contingency operations (Addressable).*
 - *Facility security plan (Addressable).*
 - *Access control and validation procedures (Addressable).*
 - *Maintenance records (Addressable).*
- Workstation use (Required)
- Workstation security (Required)
- Device and media controls
 - *Disposal (Required).*
 - *Media re-use (Required).*
 - *Accountability (Addressable).*
 - *Data backup and storage (Addressable).*

Technical Safeguard Standards:

- Access control
 - *Unique user identification (Required).*
 - *Emergency access procedure (Required).*
 - *Automatic logoff (Addressable).*
 - *Encryption and decryption (Addressable).*
- Audit controls (Required)
- Integrity
 - *Mechanism to authenticate electronic protected health information (Addressable)*
- Person or entity authentication (Required)
- Transmission security
 - *Integrity controls (Addressable).*
 - *Encryption (Addressable).*